Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for facilitating remote access by a mail client to a mail server via an intermediary server, said method comprising:

(a) receiving a mail access request at the intermediary server, the mail access request being sent to the intermediary server from the mail client for a requestor;

(b) receiving a password associated with the mail access request;

(c) authenticating the requestor with the mail server based on the received password;

~~(d) authenticating the requestor with an authentication server based on the received password, the authentication server being coupled to or within a private network that includes the mail server~~

(dl) retrieving a previously stored hashed password associated with the requestor or the mail client;

(d2) determining whether a hashed version of the received password matches the retrieved hashed password;

(d3) authenticating, based on the received password, the requestor with an authentication server that couples to a private network that includes the mail server; and

(d4) bypassing said authenticating (d3) and deeming the received password authenticated when said determining (d2) determines that the hashed version of the received password matches the retrieved hashed password.

~~(e) permitting the mail access request when both the mail server and the authentication server authenticate the requestor.~~

2. (currently amended) A method as recited in claim 1, wherein a mail server password and an authentication server password are included in or derived from the received password,

wherein said authenticating (c) authenticates the requestor with the mail server using the mail server password, and

wherein said authenticating [[(d)]] (d3) authenticates the requestor with the authentication server using the authentication server password.

3. (canceled)

4. (currently amended) A method as recited in claim [[3]] 1, wherein a mail server password and an authentication server password are ~~included in or derived from~~ separated by a password separator in the received password,

wherein said authenticating (c) authenticates the requestor with the mail server using the mail server password, and

wherein said authenticating [[(d)]] (d3) authenticates the requestor with the authentication server using the authentication server password.

5. (currently amended) A method as recited in claim [[3]] 1, wherein said retrieving (dl) further includes at least retrieving a time last authorized by the authentication server, and

wherein said method further comprises:

(d5) determining whether the time last authorized by the authentication server exceeds a predetermined duration; and

(d6) preventing said bypassing (d4) from bypassing said authenticating (d3) when said determining (d5) determines that the time last authorized by the authentication server exceeds the predetermined duration.

6. (previously presented) A method as recited in claim 5, wherein the predetermined duration is a maximum session duration.

7. (currently amended) A method as recited in claim 5, wherein a mail server password and an authentication server password are included in or derived from the received password,

wherein said authenticating (c) authenticates the requestor with the mail server using the mail server password, and

wherein said authenticating [[(d)]] (d3) authenticates the requestor with the authentication server using the authentication server password.

8. (currently amended) A method as recited in claim [[3]] 1,

wherein said retrieving (dl) further includes at least retrieving a time last used password, and

wherein said method further comprises:

(d5) determining whether the time last used password exceeds a predetermined duration; and

(d6) preventing said bypassing (d4) from bypassing said authenticating (d3) when said determining (d5) determines that the time last used password exceeds the predetermined duration.

9. (previously presented) A method as recited in claim 8, wherein the predetermined duration is a maximum idle duration.

10. (currently amended) A method as recited in claim 9, wherein a mail server password and an authentication server password are included in or derived from the received password,

wherein said authenticating (c) authenticates the requestor with the mail server using the mail server password, and

wherein said authenticating [[(d)]] (d3) authenticates the requestor with the authentication server using the authentication server password.

11. (previously presented) A method for authenticating a requestor of a remote mail client seeking access to a mail server, said method comprising:

(a) receiving a password from the remote mail client;

(b) retrieving a previously stored hashed password;

(c) determining whether a hashed version of the received password matches the previously stored hashed password;

(d) authenticating the requestor with the mail server based on the received password; and

(e) further authenticating the requestor with an authentication server based on the received password when said determining (c) determines that the hashed version of the received

password does not match the previously stored hashed password, the authentication server couples to or resides on a private network that includes the mail server.

12. (original) A method as recited in claim 11, wherein the received password is an authentication password, and wherein the authentication password serves to authenticate the requestor or the remote mail client to the authentication server.

13. (previously presented) A method as recited in claim 11,

wherein said receiving (a) further receives a time last authorized by the authentication server,

wherein said determining (c) further determines whether a time since the time last authorized by the authentication server exceeds a predetermined duration, and

wherein said authenticating (e) is performed when said determining (c) determines that the time since the time last authorized by the authentication server exceeds the predetermined duration, regardless of whether said determining (c) determines that the hashed version of the received password matches the previously stored hashed password.

14. (previously presented) A method as recited in claim 11,

wherein said receiving (a) further receives a time last used password,

wherein said determining (c) further determines whether a time since the time last used password exceeds a predetermined duration, and

wherein said authenticating (e) is performed when said determining (c) determines that the time since the time last used password exceeds the predetermined duration, regardless of

whether said determining (c) determines that the hashed version of the received password matches the previously stored hashed password.

15. (previously presented) A method as recited in claim 11,

wherein said receiving (a) further receives a time last authorized by the authentication server and a time last used password,

wherein said determining (c) further determines whether a time since the time last authorized by the authentication server exceeds a first predetermined duration and whether the time since the time last used password exceeds a second predetermined duration, and

wherein said authenticating (e) is performed when said determining (c) determines that the time since the time last authorized by the authentication server exceeds the first predetermined duration or that the time since the time last used password exceeds the second predetermined duration, regardless of whether said determining (c) determines that the hashed version of the received password matches the previously stored hashed password.

16. (original) A method as recited in claim 15, wherein the received password is an authentication password, and wherein the authentication password serves to authenticate the requestor or the remote mail client to the authentication server.

17. (original) A method as recited in claim 15, wherein the first predetermined duration is a maximum session duration, and wherein the second predetermined duration is a maximum idle duration.

18. (currently amended) A computer readable storage medium including at least computer program code for facilitating remote access by a mail client to a mail server via an intermediary server, said computer readable storage medium comprising:

computer program code for receiving a mail access request at the intermediary server, the mail access request being sent to the intermediary server from the mail client for a requestor;

computer program code for receiving a password associated with the mail access request;

computer program code for authenticating the requestor with the mail server based on the received password;

computer program code for ~~authenticating the requestor~~ retrieving a previously stored hashed password associated with the requestor or the mail client and determining whether the retrieved hashed password matches a hashed version of the received password;

computer program code for authenticating the requestor with an authentication server based on the received password, the authentication server being coupled to or included in a private network that includes the mail server; and

computer program code for bypassing the authenticating with the authentication server and deeming the received password as authenticated when the hashed version of the received password matches the retrieved hashed password.

~~computer program code for permitting the mail access request when both the mail server and the authentication server authenticate the requestor.~~

19. (previously presented) A computer readable storage medium as recited in claim 18, wherein a mail server password and an authentication server password are included in or derived from the received password,

wherein said computer program code for authenticating operates to authenticate the requestor with the mail server using the mail server password, and

wherein said computer program code for authenticating operates to authenticate the requestor with the authentication server using the authentication server password.

20. (canceled)

21. (previously presented) A computer readable storage medium including at least computer program code for authenticating a requestor of a remote mail client seeking access to a mail server, said computer readable storage medium comprising:

computer program code for receiving a password from the remote mail client;

computer program code for retrieving a previously stored hashed password;

computer program code for determining whether a hashed version of the received password matches the previously stored hashed password;

computer program code for authenticating the requestor with the mail server based on the received password; and

computer program code for authenticating the requestor with an authentication server based on the received password when said computer program code for determining determines that the hashed version of the received password does not match the previously stored hashed password, the authentication server on a private network that includes the mail server.

22. (previously presented) A computer readable storage medium as recited in claim 21, wherein the received password is an authentication password, and wherein the authentication

password serves to authenticate the requestor or the remote mail client to the authentication server.

23. (previously presented) A computer readable storage medium as recited in claim 21,

wherein said computer program code for receiving further receives a time last authorized by the authentication server,

wherein said computer program code for determining further determines whether a time since the time last authorized by the authentication server exceeds a predetermined duration, and

wherein the authenticating is performed by said computer program code for authenticating when said computer program code for determining determines that the time since the time last authorized by the authentication server exceeds the predetermined duration, regardless of whether said computer program code for determining determines that the hashed version of the received password matches the previously stored hashed password.